Certified Tech Developer

The Ultimate Degree

Introducción a la informática

Amenazas Infomáticas

Práctica integradora.

Grupo 3
Adbala, Satiago
Barragan, Yesid
Pasqualis, Agustina
Sueldo, Simón

Práctica Integradora

Objetivo

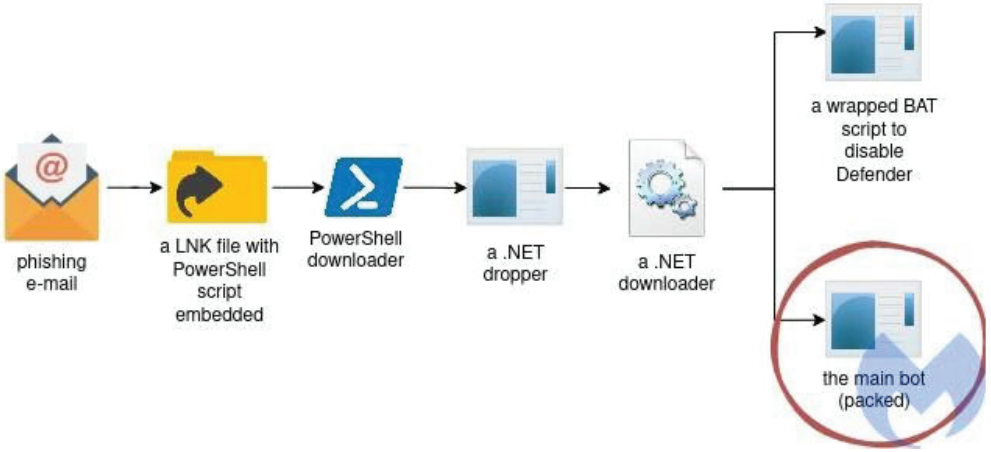
Vamos a poner en práctica los conocimientos que hemos adquirido hasta el momento. Se crearán 10 grupos, divididos en sus respectivas salas y realizarán la siguiente ejercitación.

Micro desafíos

Deberán leer cada una de la siguiente noticia y responder las siguientes consignas:

- ¿Qué tipo de amenaza es?
  Saint Bot es malware nuevo, que ha sido reportado en ataques de phishing para implementar ladrones de credenciales y otras cargas útiles maliciosas.
  Saint Bot es un troyano downloader recientemente observado que contiene el malware Taurus Stealer y Glupteba. A pesar de ser relativamente nuevo, utiliza una serie de técnicas avanzadas, lo que sugiere que sus creadores son más sofisticados de lo esperado.

- ¿Cómo comienza y cómo se propaga esta amenaza?
  La cadena de infección comienza con un correo electrónico de phishing que contiene un archivo ZIP incrustado ("bitcoin.zip") que dice ser una billetera bitcoin cuando, de hecho, es un script de PowerShell bajo la apariencia de un archivo de acceso directo .LNK. Este script de PowerShell luego descarga el malware de la siguiente etapa, un ejecutable de WindowsUpdate.exe, que, a su vez, suelta un segundo ejecutable (InstallUtil.exe) que se encarga de descargar dos ejecutables más llamados def.exe y putty.exe.
  Mientras que el primero es un script por lotes responsable de deshabilitar Windows Defender, putty.exe contiene la carga útil maliciosa que finalmente se conecta a un servidor de comando y control (C2) para su posterior explotación.



- ¿Hay más de una amenaza aplicada?

Los troyanos se pueden utilizar para robar información financiera o instalar amenazas como virus y ransomware. La información puede información robada puede ser compartida o vendidas en la Deep Web.